APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,524	03/31/2004	Kenneth E. Nicholas	200313756-1	6916

22879   7590   01/29/2009
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER
ALMEIDA, DEVIN E

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
01/29/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>02 January 2009</u>.

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1,3,4,7-15,17-20,22-24,26-31 and 33-39</u> is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1,3,4,7-15,17-20,22-24,26-31 and 33-39</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☐ All b) ☐ Some * c) ☐ None of:

   1. ☐ Certified copies of the priority documents have been received.

   2. ☐ Certified copies of the priority documents have been received in Application No. _____.

   3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 1/02/2009.

Response to Arguments

Applicant's arguments with respect to not teaching "a database storing registered biometric data associated with a plurality of biometries of the user, configuration data associated with a plurality of communication network configuration settings, and relational data relating each of the plurality of registered biometrics with corresponding ones of the communication network configuration settings" have been considered but are not persuasive.

Itoh teaches in paragraphs 0016 and 0044-0048 "pre-registering information about a communication adapter to be enabled in response to a predetermined condition of an operating environment of the computer apparatus; detecting event information generated by a change in the operating environment of the computer apparatus; analyzing the event information to determine whether the event information meets the predetermined condition of the operating environment or not; and, if the event information meets the predetermined condition of the operation environment, enabling a communication adapter to be enabled in response to the predetermined condition of the operating environment". Examples of predetermined condition can be the depression of a predetermined key. Raaf teaches a database storing registered biometric data associated with a plurality of biometries of the user (see Raaf page 3 the stored pieces of fingerprint information correspond either to different fingers of a person),

configuration data associated with a plurality of communication network configuration

settings, and relational data relating each of the plurality of registered biometrics with

corresponding ones of the communication network configuration settings' (see Raaf

page 3 the determination of the closest sample vector 'f4' for a feature 'fe', which

corresponds to the captured sensor data thus causes a corresponding control

procedure 'stp4' to be triggered). The combination of Itoh and Raaf teach all the

limitation of the claimed invention by simple incorporating the use of a biometric data of

a user instead of the depression of a predetermined key to change the communication

adapter.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of
matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the
conditions and requirements of this title.

Claims 19, 20, 22-24, 26-29 are rejected under 35 U.S.C. 101 based on

Supreme Court precedent and recent Federal Circuit decisions, a 35 U.S.C § 101

process must (1) be tied to a particular machine or (2) transform underlying subject

matter (such as an article or materials) to a different state or thing. In re Bilski et al, 88

USPQ 2d 1385 CAFC (2008); Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v.

Flook, 437 U.S. 584, 588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972);

Cochrane v. Deener, 94 U.S. 780,787-88 (1876).

An example of a method claim that would not qualify as a statutory process

would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory

process, the claim should positively recite the particular machine to which it is tied, for

example by identifying the apparatus that accomplishes the method steps, or positively

recite the subject matter that is being transformed, for example by identifying the

material that is being changed to a different state.

Here, applicant's method steps are not tied to a particular machine and do not

perform a transformation. Thus, the claims are non-statutory.

The mere recitation of the machine in the preamble with an absence of a

machine in the body of the claim fails to make the claim statutory under 35 USC 101.

Note the Board of Patent Appeals Informative Opinion Ex parte Langemyer et al.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3, 4, 7-11, 14, 15, 18-20, 22-24, 26, 27, 30, 31 and 33-37 are rejected

under 35 U.S.C. 103(a) as being unpatentable over Itoh et al (2002/0072391) in view of

Raaf (DE 198 37 642 C1).

With respect to claim 1, Itoh teaches

a configuration module adapted to automatically select a communication network

configuration setting for a device based on the depression of a predetermined key (see

paragraph 0016 and 0044-0048), wherein the configuration module is adapted to display an interface to the user identifying the registered depression of a predetermined key associated with the selected communication network configuration setting (see figure 8 and paragraph 0058).

Itoh does not teach a biometric configuration management system, comprising: a biometric sensor module for receiving biometric data associated with a user or that the predetermined key is biometric data associated with the user and a database storing registered biometric data associated with a plurality of biometries of the user, configuration data associated with a plurality of communication network configuration settings, and relational data relating each of the plurality of registered biometrics with corresponding ones of the communication network configuration settings.

Raaf teaches a biometric configuration management system, comprising: a biometric sensor module for receiving biometric data associated with a user (see Raaf page 3 as a function of the results of the comparison when the stored fingerprint information 'f4' is similar to the determined fingerprint information 'fe' the control procedure 'stp4' associated with this stored fingerprint information 'f4' is triggered and page 4) and a database storing registered biometric data associated with a plurality of biometries of the user (see Raaf page 3 the stored pieces of fingerprint information correspond either to different fingers of a person), configuration data associated with a plurality of communication network configuration settings, and relational data relating each of the plurality of registered biometrics with corresponding ones of the communication network configuration settings (see Raaf page 3 the determination of the

closest sample vector 'f4' for a feature 'fe', which corresponds to the captured sensor data thus causes a corresponding control procedure 'stp4' to be triggered and according to Itoh the control procedure can be selecting a communication network configuration setting).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used fingerprint information to allow a quick and reliable way to implement different control procedures (see Raaf page 2-3). Therefore one would have been motivated to have used a fingerprint to automatically select a one of a plurality of different communication networks for the device based on the received biometric data.

With respect to claim 2, comprising relational data accessible by the configuration module for correlating the received biometric data to the selected network configuration setting (see Itoh paragraph 0016 and 0044-0048 and Raaf page 3 and 4).

With respect to claim 3. The system of claim 1, wherein the selected communication network configuration setting comprises at least one of the group consisting of a local area network (LAN) configuration setting, a wide area network (WAN) configuration setting, a personal area network (PAN) configuration setting and a virtual private network (VPN) configuration setting (see Itoh paragraph 0005).

With respect to claim 4 configuration module is adapted to automatically switch the device to the selected communication network configuration setting from another communication network configuration setting based on the received biometric data and the relational data (see paragraph 0016 and 0044-0048).

With respect to claim 7, wherein the biometric data comprises at least one of the group consisting of a fingerprint scan biometric, a voice scan biometric, a facial feature biometric, and an eye scan biometric (see Raaf page 3 i.e. fingerprint sensor).

With respect to claim 8, wherein the configuration module is adapted to receive a selection from the user of one of the communication network configuration settings to associate with a corresponding biometric data of the user (see Raaf page 3).

With respect to claim 9 configuration module is adapted to display an interface to the users identifying registered biometrics (see figure 8 and paragraph 0058)

With respect to claim 10, wherein the configuration module is adapted to request from the user a particular biometric to associate with one of the communication network configuration setting (see Raaf page 3-4).

With respect to claim 11, wherein the selected communication network configuration setting comprises a wireless network configuration setting (see Itoh paragraph 0005).

With respect to claim 14, Itoh teaches means for automatically select a communication network configuration setting for a device based on the depression of a predetermined key (see paragraph 0016 and 0044-0048), wherein the configuration module is adapted to display an interface to the user identifying the depression of a predetermined key associated with the network configuration setting (see figure 8 and paragraph 0058).

Itoh does not teach a biometric configuration management system, comprising: means for receiving biometric data associated with a user or that the predetermined key

is biometric data associated with the user and means for storing registered biometric

data associated with a plurality of biometries of the user, configuration data associated

with a plurality of communication network configuration settings, and relational data

relating each of the plurality of registered biometrics with corresponding ones of the

communication network configuration settings.

Raaf teaches a biometric configuration management system, comprising: a

biometric sensor module for receiving biometric data associated with a user (see Raaf

page 3 as a function of the results of the comparison when the stored fingerprint

information 'f4' is similar to the determined fingerprint information 'fe' the control

procedure 'stp4' associated with this stored fingerprint information 'f4' is triggered and

page 4) and means for storing registered biometric data associated with a plurality of

biometries of the user (see Raaf page 3 the stored pieces of fingerprint information

correspond either to different fingers of a person), configuration data associated with a

plurality of communication network configuration settings, and relational data relating

each of the plurality of registered biometrics with corresponding ones of the

communication network configuration settings (see Raaf page 3 the determination of the

closest sample vector 'f4' for a feature 'fe', which corresponds to the captured sensor

data thus causes a corresponding control procedure 'stp4' to be triggered and according

to Itoh the control procedure can be selecting a communication network configuration

setting).

It would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains to have used

fingerprint information to allow a quick and reliable way to implement different control

procedures (see Raaf page 2-3). Therefore one would have been motivated to have

used a fingerprint to automatically select a one of a plurality of different communication

networks for the device based on the received biometric data.

With respect to claim 15, further comprising means for identifying to the user a

particular registered biometric associated with the selected communication network

configuration setting (see page 2 i.e. different pieces of fingerprint information

corresponding to one finger each of various persons is stored each piece of information

being associated with a control procedure).

With respect to claim 17, further comprising means for automatically switching

the device to the selected communication network configuration setting from another

communication network configuration setting based on the received biometric data and

the relational data (see Itoh paragraph 0016 and 0044-0048 and Raaf page 3 and 4)..

With respect to claim 18, further comprising means for requesting from the user a

particular biometric to associate with one of the communication network configuration

setting (see Raaf page 3).

With respect to claim 19, Itoh teaches automatically selecting a communication

network configuration setting for a device based on the depression of a predetermined

key (see paragraph 0016 and 0044-0048), wherein the configuration module is adapted

to display an interface to the user identifying the depression of a predetermined key

associated with the network configuration setting (see figure 8 and paragraph 0058)

Itoh does not teach a biometric configuration management system, comprising: receiving biometric data associated with a user or that the predetermined key is biometric data associated with the user and storing registered biometric data associated with a plurality of biometries of the user, configuration data associated with a plurality of communication network configuration settings, and relational data relating each of the plurality of registered biometrics with corresponding ones of the communication network configuration settings.

Raaf teaches a biometric configuration management system, comprising: a biometric sensor module for receiving biometric data associated with a user (see Raaf page 3 as a function of the results of the comparison when the stored fingerprint information 'f4' is similar to the determined fingerprint information 'fe' the control procedure 'stp4' associated with this stored fingerprint information 'f4' is triggered and page 4) and a database storing registered biometric data associated with a plurality of biometries of the user (see Raaf page 3 the stored pieces of fingerprint information correspond either to different fingers of a person), configuration data associated with a plurality of communication network configuration settings, and relational data relating each of the plurality of registered biometrics with corresponding ones of the communication network configuration settings (see Raaf page 3 the determination of the closest sample vector 'f4' for a feature 'fe', which corresponds to the captured sensor data thus causes a corresponding control procedure 'stp4' to be triggered and according to Itoh the control procedure can be selecting a communication network configuration setting).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used fingerprint information to allow a quick and reliable way to implement different control procedures (see Raaf page 2-3). Therefore one would have been motivated to have used a fingerprint to automatically select a one of a plurality of different communication networks for the device based on the received biometric data.

With respect to claim 20. The method of claim 19, further comprising identifying to the user a particular biometric associated with the selected communication network configuration setting (see page 2 i.e. different pieces of fingerprint information corresponding to one finger each of various persons is stored each piece of information being associated with a control procedure).

With respect to claim 22, further comprising automatically switching the device to the selected communication network configuration setting from another communication network configuration setting based on the received biometric data and the relational data (see Itoh paragraph 0016 and 0044-0048).

With respect to claim 23, wherein receiving biometric data comprises receiving at least one of the group consisting of fingerprint scan biometric data, voice scan biometric data, facial feature biometric data, and eye scan biometric data (see Raaf page 3 i.e. fingerprint sensor).

With respect to claim 24, further comprising requesting a selection from the user of one of the communication network configuration settings to associate with a corresponding biometric of the user.

With respect to claim 26, further comprising requesting from the user a particular biometric to associate with one of the communication network configuration settings (see page 2 i.e. different pieces of fingerprint information corresponding to one finger each of various persons is stored each piece of information being associated with a control procedure).

With respect to claim 27, wherein automatically selecting a communication network configuration setting comprises automatically selecting a wireless communication network configuration setting (see Itoh paragraph 0016 and 0044-0048).

With respect to claim 30, Itoh teaches a configuration module adapted to automatically select a communication network configuration setting for a device based on the depression of a predetermined key (see paragraph 0016 and 0044-0048), wherein the configuration module is adapted to display an interface to the user identifying the depression of a predetermined key associated with the network configuration setting (see figure 8 and paragraph 0058)

Itoh does not teach a biometric configuration management system, comprising: a biometric sensor module for receiving biometric data associated with a user or that the predetermined key is biometric data associated with the user and a database storing registered biometric data associated with a plurality of biometries of the user, configuration data associated with a plurality of communication network configuration settings, and relational data relating each of the plurality of registered biometrics with corresponding ones of the communication network configuration settings.

Raaf teaches a biometric configuration management system, comprising: a

biometric sensor module for receiving biometric data associated with a user (see Raaf

page 3 as a function of the results of the comparison when the stored fingerprint

information 'f4' is similar to the determined fingerprint information 'fe' the control

procedure 'stp4' associated with this stored fingerprint information 'f4' is triggered and

page 4) and and a database storing registered biometric data associated with a plurality

of biometries of the user (see Raaf page 3 the stored pieces of fingerprint information

correspond either to different fingers of a person), configuration data associated with a

plurality of communication network configuration settings, and relational data relating

each of the plurality of registered biometrics with corresponding ones of the

communication network configuration settings (see Raaf page 3 the determination of the

closest sample vector 'f4' for a feature 'fe', which corresponds to the captured sensor

data thus causes a corresponding control procedure 'stp4' to be triggered and according

to Itoh the control procedure can be selecting a communication network configuration

setting).

It would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains to have used

fingerprint information to allow a quick and reliable way to implement different control

procedures (see Raaf page 2-3). Therefore one would have been motivated to have

used a fingerprint to automatically select a one of a plurality of different communication

networks for the device based on the received biometric data.

With respect to claim 31, wherein the configuration module is adapted to receive a selection from the user of one of the communication network configuration settings to associate with a corresponding biometric of the user (see Raaf page 2 i.e. different pieces of fingerprint information corresponding to one finger each of various persons is stored each piece of information being associated with a control procedure).

With respect to claim 33, wherein the configuration module is adapted to display a purity of available communication network configuration setting to the user for associating with the corresponding biometric of the user (see Itoh figure 8 and paragraph 0058).

With respect to claim 34, wherein the configuration module is adapted to associate with one of the communication network configuration setting at least one of the group consisting of a fingerprint scan biometric, a voice scan biometric, a facial feature biometric, and an eye scan biometric (see Raaf page 3 i.e. fingerprint sensor).

With respect to claim 35, wherein the configuration module is adapted to display to the user biometrics registered with particular communication network configuration settings (See Raaf page 3 and 4 and Itoh figure 8 and paragraph 0058).

With respect to claim 36, wherein the configuration module is adapted to request from the user a particular biometric to associate with a corresponding one of the network configuration settings (see page 2 i.e. different pieces of fingerprint information corresponding to one finger each of various persons is stored each piece of information being associated with a control procedure).

With respect to claim 37, wherein the configuration module is adapted to associate a wireless communication network configuration setting for the device with the biometric data (see page 2 i.e. different pieces of fingerprint information corresponding to one finger each of various persons is stored each piece of information being associated with a control procedure).

Claims 12, 13, 28, 29, 38, 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Itoh et al (2002/0072391) in view of Raaf (DE 198 37 642 C1) in further view of Topping (2004/0151353). Itoh and Raaf teaches everything with respect to claim 1, 29, and 30 above but with respect to claims 13, 29 and 39 he does not teach wherein the received biometric data comprises a plurality of sequentially input biometrics. Topping teaches wherein the received biometric data comprises a plurality of sequentially input biometrics (see Topping paragraph 0017 and 0032). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have requires several fingerprints to be entered in a particular sequence to further increase system security (see Topping paragraph 0017). Therefore one would have been motivated to have input a plurality of sequentially input biometrics to increase system security.

With respect to claim 12, 28 and 38, wherein the received biometric data comprises a plurality of simultaneously input biometrics (see Topping paragraph claim 13).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Devin Almeida/

Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432